

**TO: Clerk's Office
UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK**



**APPLICATION FOR LEAVE
TO FILE DOCUMENT UNDER SEAL**

In the Matter of a Search and Seizure
Warrant for a Premises Located in Brooklyn,
New York 11213, and Any Closed
Containers/Items
Contained Therein

23-MJ-967

Docket Number

SUBMITTED BY: Plaintiff ___ Defendant ___ DOJ ☒
Name: Philip Pilmar
Firm Name: USAO EDNY
Address: 271 Cadman Plaza E
Brooklyn, NY 11201
Phone Number: 718-254-6106
E-Mail Address: philip.pilmar@usdoj.gov

INDICATE UPON THE PUBLIC DOCKET SHEET: YES ___ NO ☒

If yes, state description of document to be entered on docket sheet:

MANDATORY CERTIFICATION OF SERVICE:

A.) ___ A copy of this application either has been or will be promptly served upon all parties to this action, B.) ___ Service is excused by 31 U.S.C. 3730(b), or by the following other statute or regulation: _____; or C.) ☒ This is a criminal document submitted, and flight public safety, or security are significant concerns. (Check one)

November 1, 2023
DATE

P. Pilmar
SIGNATURE

A) If pursuant to a prior Court Order:

Docket Number of Case in Which Entered: _____

Judge/Magistrate Judge: _____

Date Entered: _____

B) If a new application, the statute, regulation, or other legal basis that authorizes filing under seal

ongoing investigation

**ORDERED SEALED AND PLACED IN THE CLERK'S OFFICE,
AND MAY NOT BE UNSEALED UNLESS ORDERED BY
THE COURT.**

DATED: Brooklyn, NEW YORK
November 1, 2023

Lois Bloom

Type text here

U.S. MAGISTRATE JUDGE

RECEIVED IN CLERK'S OFFICE November 1, 2023
DATE

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

In the Matter of the Application of the United States Of America for a Search and Seizure Warrant for the Premises Known and Described as [REDACTED] Brooklyn, New York 11213, and Any Closed Containers/Items Contained Therein

TO BE FILED UNDER SEAL
APPLICATION FOR A SEARCH
WARRANT
Case No. 23-MJ-967

AFFIDAVIT IN SUPPORT OF AN
APPLICATION UNDER RULE 41 FOR A
WARRANT TO SEARCH AND SEIZE

I, [REDACTED], being first duly sworn, hereby depose and state as follows:

I. Introduction

A. Affiant

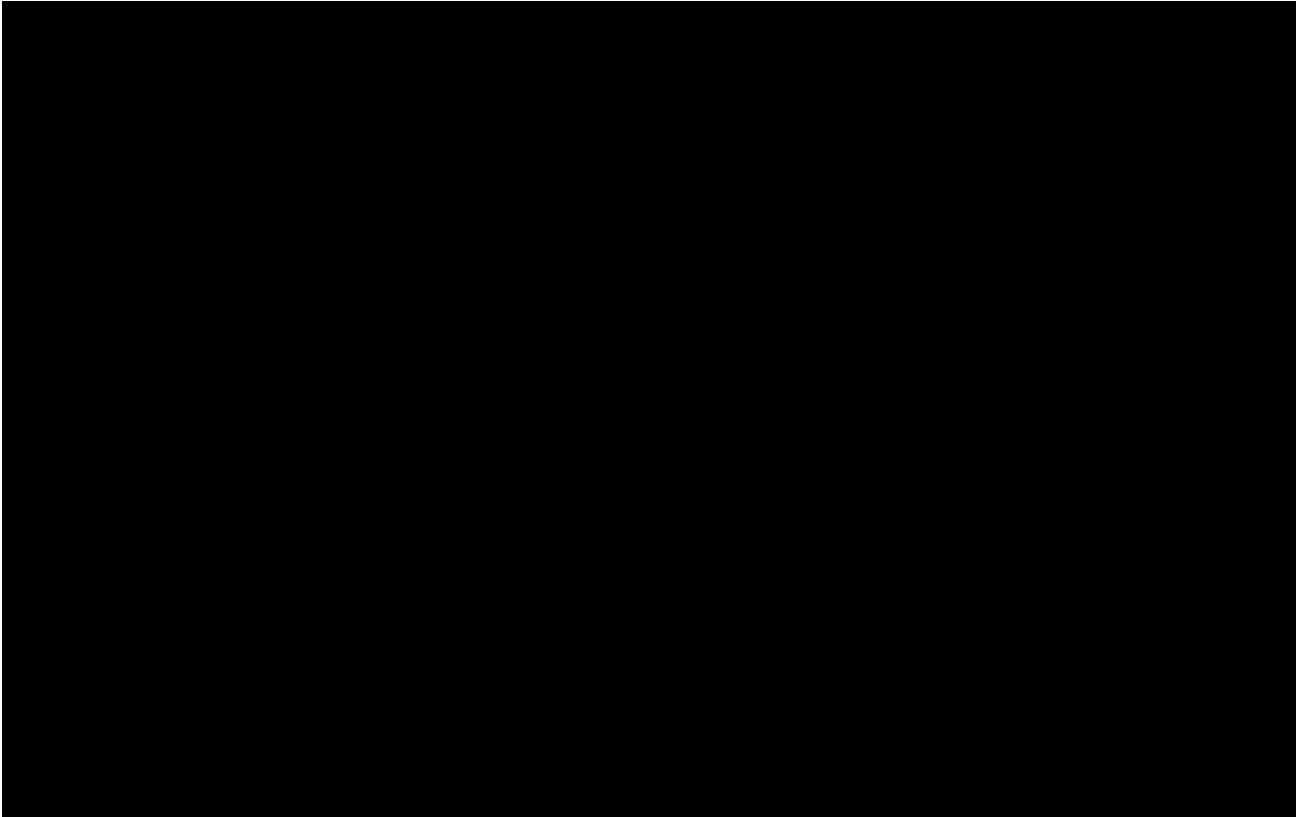
1. I have been a Special Agent with the Federal Bureau of Investigation (“FBI”) since 2019. I am currently assigned to a public corruption squad of the New York Field Office, where, among other things, I investigate crimes involving illegal campaign contributions, theft of federal funds, and bribery. Through my training and experience, I also have become familiar with some of the ways in which individuals use smart phones and electronic communications, including social media, email, and electronic messages, in furtherance of their crimes, and have participated in the execution of search warrants involving electronic evidence.

2. I make this Affidavit in support of an application pursuant to Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the premises specified below and in Attachment A (the “Subject Premises”) for, and to seize, the items and information described in Attachment B. This affidavit is based upon my personal knowledge; my review of documents and other evidence; my conversations with other law enforcement personnel; and my training,

experience and advice received concerning the use of computers in criminal activity and the forensic analysis of electronically stored information (“ESI”). Because this affidavit is being submitted for the limited purpose of establishing probable cause, it does not include all the facts that I have learned during the course of my investigation. Where the contents of documents and the actions, statements, and conversations of others are reported herein, they are reported in substance and in part, except where otherwise indicated.

B. The Subject Premises

3. The Subject Premises is particularly described as [REDACTED] Brooklyn, New York 11213. [REDACTED] is a three-story limestone building, accessed via windowed double doors up a flight of stairs from the sidewalk, with the number “[REDACTED]” inscribed on a diagonal to the left of the doors. The building, and a close-up of the doorway to the Subject Premises, are depicted below.



C. The Subject Offenses

4. For the reasons detailed below, I respectfully submit that there is probable cause to believe that the Subject Premises contains evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Section (i) 18 U.S.C. §§ 371 and 666 (theft of federal funds and conspiracy to steal federal funds), (ii) 18 U.S.C. §§ 1343 and 1349 (wire fraud and attempt and conspiracy to commit wire fraud), and (iii) 18 U.S.C. § 371 and 52 U.S.C. § 30121 (campaign contributions by foreign nationals and conspiracy to commit the same) (collectively, the “Subject Offenses”).

II. Probable Cause

A. Probable Cause Regarding Subjects’ Commission of the Subject Offenses

5. Since in or about August 2021, the FBI and the Office of the United States Attorney for the Southern District of New York have been investigating the possible receipt of so-called “straw” donations by the 2021 New York City mayoral campaign of Eric Adams (the “Adams Campaign”) from employees of [REDACTED] a construction company that operates in New York City.¹ Based on my review of publicly available information, among other sources, I know that [REDACTED] is affiliated with a larger Turkish company and many of its employees are Turkish nationals. As detailed more fully below, Turkey’s Consul General in New York was involved in the arrangement of a [REDACTED] fundraiser where straw donations (the “Straw Donations”) were made to the Adams Campaign, the Consul General has communicated about this matter with [REDACTED], a member of Adams’ staff, and Adams has communicated with [REDACTED] about fundraising in the Turkish community and the potential provision of benefits to

¹ A straw, or “conduit,” donation occurs when a donation to a political campaign is made in the name of one donor, but the funds in question in fact belong to a different person.

the Consul General. Adams and members of his staff have intervened in at least one matter within the purview of the New York City government to obtain favorable action for the Consul General. Adams and others associated with him also appear to have received various benefits from persons affiliated with the Consul General.

6. This application seeks a warrant to search a premises, the Subject Premises, including electronic devices found therein, used by [REDACTED]. From my review of publicly available information, I know that [REDACTED] worked as a fundraiser for the Adams Campaign, was employed with the Brooklyn Borough President's office when Adams was the Brooklyn Borough President, and is now a fundraiser for the Kings County Democratic Party. As detailed below, [REDACTED] was involved in coordinating the event at which the Straw Donations were made, communicating directly with [REDACTED] the Turkish Consul General [REDACTED], and a [REDACTED] employee, [REDACTED], who was involved in coordinating [REDACTED]'s involvement in fundraising for the Adams Campaign. And after the Straw Donations were made, [REDACTED] communications indicate that she traveled abroad with [REDACTED] assistance.

The Adams Campaign and New York City's Matching Funds Program

7. I understand, based on my review of publicly available information, that:

a. The Adams Campaign accepted matching funds from the New York City Campaign Finance Board throughout a significant part of its campaign ("Matching Funds"), meaning that the Adams Campaign received funds from the New York City government as a result of donations the Adams Campaign received from private donors that were eligible for matching funds.²

² See, e.g., <https://www.nyl.com/nyc/allboroughs/news/2021/10-/08/eric-adams-is-taking-a-rare-step--turning-down-campaign-cash> (reporting on the Adams Campaign's prior acceptance of matching funds and decision to turn down some matching funds as of October 7, 2021);

b. Under New York City law, the Adams Campaign was eligible to receive \$2,000 in Matching Funds, and no more than \$2,000 in Matching Funds, for each donation of \$250 from an individual donor who resides within New York City, subject to certain exceptions not relevant here. If an individual donated more than \$250, any amount in excess of \$250 would not be eligible for matching funds.³

c. New York City receives in excess of \$10,000 per year in federal funding.⁴

The Suspected Straw Donations

8. I understand, based on information provided by the New York City Campaign Finance Board, that the Adams Campaign received the following donations, among others, on May 7, 2021:

AMOUNT	NAME	CITY	STATE	OCCUPATION	EMPLOYER NAME
\$1,500	Arkan, Erden	New York	NY	Owner	[REDACTED]
\$1,200	[REDACTED]	Flushing	NY	Sr. Prod. Manager	[REDACTED]
\$1,250	[REDACTED]	Brooklyn	NY	Account Manager	[REDACTED]
\$1,250	[REDACTED]	Flushing	NY	Construction	[REDACTED]
\$1,250	[REDACTED]	Cliffside Park	NJ	Business Logistics	[REDACTED]
\$1,250	[REDACTED]	Brooklyn	NY	PM	[REDACTED]

https://www.nycffb.info/VsApps/CandidateSummary.aspx?as_cand_id=1545&as_election_cycle=2021&cand_name=Adams%2C+Eric+L&office=Mayor&report=summ (New York City Campaign Finance Board's report detailing total public funds disbursed to Adams Campaign).

³ See <https://www.nycffb.info/program/how-it-works>.

⁴ See https://comptroller.nyc.gov/wp-content/uploads/2016/11/Federal_Budget_Vulnerabilities_Memo.pdf.

\$1,250	██████████	Brooklyn	NY	Engineer/ Lawyer	██████████
\$1,250	██████████	Brooklyn	NY	Project manager	██████████
\$1,250	██████████	Ridgewood	NJ	Finance Director	██████████
\$1,250	██████████	Flushing	NY	Partner	██████████
\$1,250	██████████	New York	NY	Accountant	██████████

The individuals listed in this table are hereinafter referred to as the “Donors.”

9. I have further confirmed that, with the exception of the donations by ██████████ ██████████ and ██████████ ██████████ Matching Funds were issued in connection with each of the donations identified above.⁶

10. Bank records for ██████████ indicate that on April 28, 2021, ██████████ issued checks in the amount of \$1,250 to each of the Donors with the exception of Arkan and ██████████ and also issued a \$1,250 check to ██████████ ██████████ ██████████. I know from law enforcement databases that ██████████ is ██████████ spouse. I know from my review of emails sent to and from each of the Donors except for ██████████ and also including emails sent to and from ██████████ (collectively, the “██████████ Emails”), obtained pursuant to a search warrant, that ██████████ is also employed by ██████████. As noted above, Arkan’s donation to the Adams Campaign identifies Arkan as an or the owner of ██████████. Thus, on April 28, 2021, ██████████ paid each of the Donors the amount of their May 7, 2021 donation, with the exceptions

⁵ The description of ██████████ as an “Engineer/lawyer” at ██████████ is taken from the donation form submitted to the New York City Campaign Finance Board as part of her donation, but it appears from publicly available information that ██████████ may not in fact be employed at ██████████, although as explained in ¶ 10, her husband does appear to be employed at ██████████.

⁶ I understand that Matching Funds are only available for donations made by persons who reside in New York City, and both ██████████ and ██████████ reside in New Jersey.

of [REDACTED] whose husband instead received a check for that amount; Arkan, whose donation form describes him as the owner of [REDACTED]; and [REDACTED] who donated \$50 less to the Adams Campaign than [REDACTED] received from [REDACTED].

The [REDACTED] Emails

11. I know from my review of the [REDACTED] emails, in substance and in part, that:

a. On April 10, 2021, Arkan sent an email (the “April 10 Email”) in Turkish⁷ to seven individuals, five of whom have corporate email addresses indicating involvement in the construction industry. Arkan also copied seven [REDACTED] employees, of whom four are Donors and one of whom, [REDACTED] is the husband of a Donor. Arkan wrote, in substance and in part, that: In the previous week he had met with (then) Brooklyn Borough President Eric Adams, and the New York General Consul (who I understand, based on information discussed below, to be Turkey’s New York Consul General) also joined them; Adams is running for New York City Mayor and has warm feelings for Turkish business people; Arkan knows that the recipients of the email have been supporting Adams so far, but “they” (from context, [REDACTED]) are organizing a very special event in Arkan’s office on May 5th, between 5 and 6:30 pm; the recipients of the email should participate in the event and contribute; this may “feel like swimming against the current” but unfortunately, this is how things are done in this country; and this will hopefully be a successful fundraising event.

b. On April 21, 2021, Arkan sent an email to four individuals to thank them all for participating in an unspecified event. Arkan further wrote that in the morning, he had

⁷ Many of the [REDACTED] emails, as well as other communications below, are written wholly or partly in Turkish. I have reviewed draft summaries of those emails prepared by a Turkish linguist employed by the FBI, which are reflected in this Affidavit. Quotations to these emails are to the summaries prepared by the linguist.

spoken with “Consul General [REDACTED],” who was very happy and thought that mid-May would be an appropriate target date. I know from publicly available materials that [REDACTED] [REDACTED] is the consul general of Turkey’s New York consulate.

c. On April 21, 2021, Arkan emailed [REDACTED] [REDACTED] (a Donor and [REDACTED] employee) the phone number for “[REDACTED] [REDACTED] Brooklyn Borough.”

d. On April 26, 2021, [REDACTED] emailed Arkan and stated that she had “texted” with [REDACTED] and that [REDACTED] “said the checks can [b]e made payable to: Eric Adams 2021.”

e. Also on April 26, 2021, [REDACTED] asked Arkan: “Do you want me to email all the people on our list that are capable of making contributions to find out if they are willing to do it? Also Food and beverages, who would you like me to get to cater it?” Arkan responded by forwarding [REDACTED] the April 10 Email.

f. From on or about April 27, 2021 through on or about May 7, 2021, [REDACTED] sent a series of emails inviting persons and businesses associated with [REDACTED], including the recipients of the April 10 Email, to attend a fundraiser for the Adams Campaign, which Adams personally was scheduled to attend, hosted by [REDACTED] on May 7, 2021. Arkan and [REDACTED] were consistently copied on these emails.

g. On April 27 and 28, 2021, Arkan exchanged three emails with [REDACTED], who is not a Donor but, based on his email address and the statements in his email, is a [REDACTED] employee. In the first email, [REDACTED] responds to one of the emails sent by [REDACTED] described above in paragraph 11(d), asking whether he should set up a “‘go fund me’ kind of thing and share the link with everyone” so that the group could raise funds for Adams toward a target amount using a website. Arkan replied in Turkish and only to [REDACTED] stating that it would “cramp their style” to use the method proposed by [REDACTED] Arkan further explained that “the goal is to host the

man there and to hand the checks to his secretary,” that [REDACTED] method “is too professional” and that [REDACTED] “need[s] to be hands on.” [REDACTED] replied that he would “polish his checkbook” and attend. According to other [REDACTED] Emails I have reviewed, [REDACTED] donated \$200 to the Adams Campaign.

h. On May 5, 2021, Arkan emailed [REDACTED] and [REDACTED] (another Donor and [REDACTED] employee): “Don’t forget to remind our guest for fundraising event!” Subsequently on May 5, 2021, [REDACTED] sent a “friendly reminder regarding our fundraiser with ‘Eric Adams for Mayor’” to the parties described above in paragraphs 11(a) and 11(d).

i. On May 7, 2021, shortly after the scheduled time for the fundraiser, Arkan thanked [REDACTED] [REDACTED] and [REDACTED] [REDACTED] (another Donor and [REDACTED] employee) for their hard work in making “this event” successful. Arkan copied [REDACTED] on this email. As noted above, also on May 7, 2021, the Donors made donations to the Adams Campaign that largely matched the amount of money [REDACTED] had paid them on April 28, 2021.

j. On May 10, 2021, [REDACTED] sent [REDACTED] an email with no subject heading or body, attaching a photograph of a handwritten list (the “List”). The List is entitled “Eric Adams 2021 Donation,” and consists of a column of names with corresponding dollar amounts. The List includes all of the Donors and accurately reflects the amount of their donations, except that [REDACTED] is listed as a donor of \$1,250, when according to records maintained by the New York City Board of Elections, it was [REDACTED] wife, [REDACTED] [REDACTED],⁸ who donated that amount. The List also reflects smaller donations by ten other individuals or corporations, most of whom appear to have received the emails from [REDACTED] and Arkan urging contribution that are described above in paragraphs

⁸ On the records provided by the New York City Campaign Finance Board, [REDACTED] first name is spelled “[REDACTED]” On [REDACTED] bank records as well as the underlying donation slip, however, she uses the common spelling “[REDACTED]”

11(a) and 11(d). In total, the list records \$20,000 in donations, of which nearly 70% came from the Donors.

The [REDACTED] Messages

12. Phone records indicate that between February 8, 2021 and January 14, 2022, a phone number subscribed in [REDACTED] name (the “[REDACTED] Number”) exchanged 22 calls with a phone number subscribed to the Turkish Consulate General (the “Consulate Number”).⁹ This includes a call on April 2, 2021. As explained above, in the April 10 Email, Arkan stated that he had met with the Consul General and Adams in the prior week, and planned to hold a fundraiser for Adams.

13. I have reviewed photographs posted to the Internet on November 18, 2021 by the Turkish Consulate General in New York City showing persons I believe to be [REDACTED] [REDACTED] (the Consul General), and Eric Adams together.

14. Toll records indicate that on May 19, 2021, the [REDACTED] Number and a phone number subscribed to by Arkan exchanged two calls, one of which resulted in a call of one minute and 11 seconds in duration and the other of which did not result in a listed duration (possibly indicating that the call was not answered).

15. From my review of the contents of an iCloud account and Apple iPhone used by [REDACTED] obtained pursuant to search warrants, I know that [REDACTED] exchanged messages, including over encrypted messaging applications WhatsApp and Signal, with [REDACTED] (Turkey’s Consul General in New York), [REDACTED] and [REDACTED] among others, including the following, in substance and in part:

⁹ These records are not complete, but rather do not include April 2022 and parts of March and May 2022.

a. On June 14, 2018, [REDACTED] and [REDACTED] exchanged messages concerning the legal limits for corporate donations in elections.

b. On June 28, 2018, [REDACTED] texted [REDACTED] “The list for 6/22/18,” which appears to be a list of names and dollar amounts. I know from my review of records maintained by the New York City Campaign Finance Board that this list reflects, in part, donations to the Adams Campaign, which had already begun fundraising at that time.

c. In October and November 2018, [REDACTED] and Adams exchanged text messages that appear to involve one or more meetings with individuals associated with Turkey, because, among other reasons, the messages referred to the “Group from Turkey (from yesterday meeting),” “my guy from [REDACTED],” and several names that I recognize from my experience in this case as commonly used by people of Turkish heritage. On November 6, 2018, after an event that Adams described as “Went well,” Adams told [REDACTED] “They showed me a lot of love. Lol. Let’s move to the next level.”

d. On January 13, 2021, [REDACTED] and [REDACTED] exchanged messages in which [REDACTED] sought a meeting with Adams. [REDACTED] asked [REDACTED] “what will the topic be?” [REDACTED] replied, in a series of messages, “The election,” “that’s what,” “Turkish community support to him,” and “What can we do, let’s talk.”

e. Between January 20 and February 13, 2021, [REDACTED] communicated with [REDACTED] to set up a meeting which eventually occurred on February 14, 2021, and which [REDACTED] and Adams attended.

f. On April 1, 2021, [REDACTED] sent [REDACTED] a “List of people who will attend the meeting,” which included Arkan and [REDACTED] As discussed above, the [REDACTED] Emails, among

other evidence, reflect Arkan stating that he met Adams and [REDACTED] in early April 2021, after which the events leading to the Straw Donations occurred.

g. Between April 11, 2021, and April 21, 2021, [REDACTED] and [REDACTED] exchanged messages that I believe to concern the [REDACTED] fundraiser held for the Adams Campaign on May 7, 2021, discussed above. For example, on April 15, 2021, [REDACTED] and [REDACTED] exchanged a series of proposed dates for “the event,” and settled on May 7, 2021. In response to a question from [REDACTED] about “the location,” [REDACTED] replied “[REDACTED] – Headquarters,” and supplied the phone number and a link to the address of [REDACTED].

h. On or about April 21, 2021, [REDACTED] sent [REDACTED] the following message: “Also I gave your number to one of the gentleman [*sic*] from last time dinner[.] He has questions regarding campaigns[.] His name is Erden Arkan[.]”

i. On May 7, 2021, [REDACTED] asked [REDACTED] for “forms,” stating: “They already collect the checks.” [REDACTED] responded “Yes” to [REDACTED] text asking if she had “forms.” Based on [REDACTED] status as a fundraiser for the Adams Campaign and this message being sent on the day of the [REDACTED] fundraiser at which checks for the Straw Donations were given to the Adams Campaign, I believe that in this message [REDACTED] requested contribution forms for the already-made [REDACTED] donations.

j. Between September 6 and 10, 2021, [REDACTED] and [REDACTED] exchanged a series of messages, the substance of which [REDACTED] then relayed to Adams, concerning, in substance and in part, obtaining a Temporary Certificate of Occupancy (“TCO”) for the official opening of a building associated with the Turkish Consulate in New York in time for a visit by Turkey’s president. In these messages, [REDACTED] repeatedly asked [REDACTED] to have “Eric,” who I understand to be Eric Adams, assist in obtaining a TCO from the Fire Department of New York

(“FDNY”). When ██████ relayed these requests to Adams, Adams told her that he was speaking with an unspecified person, who from context appears to be an FDNY official, and was working to “resolve this.” Adams also stated that he had spoken directly “to the council [*sic*] general,” who I understand to be ██████ on this subject. On September 10, 2021, ██████ wrote Adams “Problem was resolved[.] Thank you very much,” and Adams replied, “Anything for you ██████

k. On April 21, 2022, ██████ and ██████ exchanged a series of messages in which ██████ asked ██████ in substance, to confirm that Adams would not make “A statement about the Armenia Genocide” on the “24th of April,” and ██████ replied, “No” “He wont.” I am aware, based on my review of publicly available information, that April 24 is Armenian Genocide Remembrance Day and that the Turkish Government denies that the Armenian Genocide (which was committed by Turkey’s government between 1915 and the early 1920s) occurred. ██████ made further requests related to “the Armenians,” and ██████ replied, “We try to stop the official requests as much as we can,” and “We do not let him get into these kinds of conflicts.”

l. On July 11, 2022, ██████ encouraged ██████ to “Ask her all your pending problems regarding this building ... Like FDNY approvals.” Based on the messages detailed *supra* ¶ 15(j), I believe ██████ is referencing a building associated with the Turkish Consulate in New York.

16. From my review of the contents of an iCloud account used by ██████ obtained in August 2022 pursuant to a search warrant, I know that ██████ received and responded to some of the messages from ██████ discussed above relating to arranging the February 2021 meeting between Adams and ██████ and relating to arranging the May 2021 event at which ██████ employees made straw donations to the Adams Campaign. ██████ also had relevant communications directly

with Adams, as well as communicating directly with [REDACTED] the Turkish Consul General in New York. For instance:

a. On February 12, 2021, days before the meeting [REDACTED] coordinated with [REDACTED] to arrange between [REDACTED] and Adams, referred to in ¶ 15.e above, [REDACTED] and Adams exchanged the following messages:

Adams: Please we the Sunday Turkish meeting know can't do Saturday. I can do Sunday. Also call [REDACTED] she keeps calling me. Let her know I am on a zoom.

[REDACTED] I'm working on it

Adams: Need to catch Turkish before they shut down.

[REDACTED] I am on the phone with them

b. On April 5, 2021, a few days after the April 1, 2021 message listing attendees of "the meeting," including Arkan and [REDACTED] referred to in ¶ 15.f above, [REDACTED] wrote to [REDACTED] asking: "When you have a chance can you give me the dates for the event?" [REDACTED] responded "Hi [REDACTED] Can you please give them 5/7 at 5:00 pm-7:00 pm?" followed shortly by "Sorry 5:00 pm-6:30 pm." As noted above, May 7 is the date on which the [REDACTED] event was held and the Straw Donations were made.

c. On April 21, 2021, a few minutes before [REDACTED] message to [REDACTED] about giving [REDACTED] number to Arkan, referred to in ¶ 15.h above, [REDACTED] received a series of messages on the same subject via WhatsApp from [REDACTED] [REDACTED] wrote to [REDACTED] "Hi [REDACTED] this is [REDACTED], Turkish Consul General," "I hope all is well with you and Eric," "Mr Erden Arkan will call you for some info."

d. On June 27, 2021, [REDACTED] sent another series of messages to [REDACTED] one of which said “pls check Signal messages,” and [REDACTED] responded “Hi Consul General, I’m having issues with my signal. I’m going to turn my phone off and then on to see if it gets better.”¹⁰

e. Later on June 27, 2021, [REDACTED] wrote to [REDACTED] “Is everything fine with you,” “how is hotel?” [REDACTED] responded “Everything is wonderful, thank you,” and [REDACTED] replied “enjoy your time there.”

f. On June 30, 2021, [REDACTED] and [REDACTED] exchanged messages in which [REDACTED] told [REDACTED] “I’m trying to get on my flight to enter Greece and they will not allow me to enter,” and they had an ensuing discussion about a form [REDACTED] needed to fill out that she could not complete until the following day—[REDACTED] asked [REDACTED] for “the name of the form,” she responded “It’s the PLF form,” [REDACTED] asked “you can fill the same now?” and [REDACTED] responded “It won’t allow me to fill it out now, the earliest I can fill it out is tomorrow.” Less than two hours after that exchange, [REDACTED] and [REDACTED] exchanged the following messages:

[REDACTED]	[REDACTED] told me you are in the business lounge now ¹¹
[REDACTED]	at least enjoy the day
[REDACTED]	There is always a solution, though it is not the same with mykonos lol
[REDACTED]	I will, Thank you so much for all your help!!

¹⁰ [REDACTED] iCloud does not contain Signal messages. However, based on my training and experience and my involvement in this investigation, I know that messages on Signal and other encrypted messaging applications often are not backed up to iCloud but can be recovered from the electronic devices themselves. For instance, in this investigation, law enforcement searched [REDACTED] iCloud pursuant to a search warrant, and then subsequently executed a separate search warrant on her cellphone, and the latter search warrant returned significant additional information, including Signal messages that were not stored on iCloud.

¹¹ The identity and relevance of [REDACTED] are discussed below.

17. I also know from reviewing [REDACTED] iCloud account that she had calendar entries dated June 27, 2021 and June 30, 2021—the dates of the travel-related communications with [REDACTED] discussed above—containing “[REDACTED] flight details” for travel between Istanbul, Turkey and Athens, Greece.

18. I have also reviewed communications found on [REDACTED]’s iPhone and/or her iCloud account involving or discussing [REDACTED]. I know based on my investigation of this case that [REDACTED] was an employee of [REDACTED] stationed in New York City who was involved in assisting Adams with travel to Turkey in coordination with [REDACTED] and [REDACTED] the Consul General discussed above. The [REDACTED] Messages include, among other messages, the following, in substance and in part:

a. On November 6, 2018, Adams asked [REDACTED] for the name of “my guy from [REDACTED] again” and [REDACTED] replied with [REDACTED]’s first name.

b. In January 2019, [REDACTED] exchanged messages with [REDACTED] arranging Adams’ travel to Turkey, and then sent Adams his itinerary for a vacation in Turkey.

c. On September 22, 2019, [REDACTED] wrote to Adams that “your brother [REDACTED] [REDACTED] first name]. . . needs your help” and Adams told [REDACTED] to call.

d. On April 2, 2021, [REDACTED] sent [REDACTED] “the names of the individuals, who’ll attend the dinner on April the 2nd” followed by a list of names including Arkan’s. Based on the date and the individuals named in attendance, I believe this is the same early April 2021 dinner described above, which was also attended by Adams and [REDACTED] and which appears to have initiated the events leading to the Straw Donations.

e. Also on April 2, 2021, [REDACTED] requested that [REDACTED] “upgrade my ticket.” [REDACTED] replied “Again?” followed by a smiley face emoji, and later sent what appears to be an airline

reservation code. This message is consistent with a series of messages involving █████ showing that █████ often provided free upgrades of airline travel by Adams, █████ and others associated with Adams.

f. Between June 2021 and November 2021, █████ and █████ exchanged a series of messages planning travel in Turkey for Adams. Messages between █████ and █████ stressed Adams' desire that travel in November 2021 be conducted secretly. In addition, on November 29, 2021, █████ wrote █████ "Don't let █████ [first name] fool him, we are the state."

g. On June 25, 2021, █████ wrote █████ inquiring about where Adams should stay while in Turkey. █████ suggested the "Four Seasons," a luxury hotel. █████ responded "it's too expensive." █████ replied, "what's it to him . . . he is not going to pay . . . there will not . . . be a name either . . . anywhere."¹²

19. From my review of an iCloud account used by Eric Adams (the "Adams iCloud Account"), obtained pursuant to a search warrant, I know that the Adams iCloud Account contains an undated note listing numerous persons and entities, many associated or potentially associated with fundraising. That list includes the following entries: "█████ – █████" and "Turkish consultant general" and "do a turkish fundraiser with counsel general" Based on my training, experience, and participation in this investigation, I understand "█████ – █████" to refer to █████,¹³ who Adams

¹² The █████ Account also contains other messages suggesting that Adams intended to pay for travel, or at least desired to create a record to that effect. June 24, 2021, █████ informed Adams that he did not have to pay, and Adams responded "I will. Let me handle it. It's all good. 😊." And on July 8, 2022, █████ wrote █████ "In the past, █████ issued the tickets. And we paid them."

¹³ I understand, based on my conversations with a Turkish linguist employed by the FBI, that █████ first name is often transliterated as "█████" but often pronounced similarly to "█████"

knows through [REDACTED] [REDACTED] and “Turkish consultant general” and “counsel general” to refer to [REDACTED] Turkey’s Consul General in New York.

20. I have also reviewed communications found on [REDACTED] iPhone and/or her iCloud account involving or discussing [REDACTED], a Turkish national who has communicated with [REDACTED] about donating funds from Turkish nationals to the Adams Campaign under false identities. For example:

a. On June 22, 2018, [REDACTED] and [REDACTED] discussed a possible trip by Adams to Turkey. In addition, [REDACTED] stated “Fund Raising in Turkey is not legal, but I think I can raise some money for your campaign off the record.” [REDACTED] inquired, “How can he declare that money here?” [REDACTED] responded “He won’t declare it . . . Or . . . We’ll make the donation through a U.S. citizen in the U.S. . . . A Turk . . . I’ll give him cash in Turkey . . . Or I’ll send it to an American . . . He can make the donation to you.” [REDACTED] replied “I don’t think he’ll get involved in such games, which might transpire into something else later on” but “I’ll ask him anyways.” Less than two minutes later,¹⁴ the following exchange occurred:

[REDACTED]	Dearest [REDACTED], how much do you think you can come up with? \$?
[REDACTED]	Max \$100K
[REDACTED]	100K? Can you bring it here? . . . We can’t do it while Eric is in TR.
[REDACTED]	Let’s think about this.

¹⁴ In the intervening portion of the conversation, [REDACTED] stated that “He,” from context, Adams, “actually asked for Ms. [REDACTED]’s assistance” and briefly discussed that topic. Based on my review of publicly available information, [REDACTED] appears to be a prominent Turkish businesswoman who has operated in the New York City area. It is at present unclear whether this exchange related to the possible contribution, or a separate subject.

b. On February 11, 2019, [REDACTED] inquired with [REDACTED] about a “fundraising event” that “the Turks” would conduct “for Eric.” [REDACTED] informed him that the event would occur on February 22 and invited him to attend.

c. On July 11, 2021, [REDACTED] and [REDACTED] discussed dates for an unnamed event. [REDACTED] also asked [REDACTED] “how much did you decide to raise/donate?” [REDACTED] replied “We should raise/donate 40-50” and “We won’t go below 50.” Shortly thereafter, the following exchange occurred:

[REDACTED]	He had mention 200K. . . Didn’t happen?
[REDACTED]	We can’t work out the number of people . . . Otherwise it’s easy
[REDACTED]	I can work out the number of people
[REDACTED]	Hmmm then great!
[REDACTED]	From what I gathered you’ll distribute the money
[REDACTED]	Yes
[REDACTED]	Not everyone has to attend the event.

d. Between October 10 and 12, 2021, [REDACTED] asked [REDACTED] “Did you get the money from [REDACTED]?” [REDACTED] stated “Only 4000.” [REDACTED] replied “Interesting . . . The rest should come.” Based on my review of publicly available information, [REDACTED] appears to refer to [REDACTED], a Washington, D.C., based university which is partners with a Turkish university named [REDACTED]. Records maintained by the New York City Campaign Finance Board indicate that on September 27, 2021, five employees of [REDACTED] donated \$2,000 each to the Adams Campaign. The Adams Campaign returned all five donations the same day they were received.

e. On April 30, 2022, [REDACTED] and [REDACTED] exchanged the following messages:

Are the accounts open for Eric's election campaign?

Hello dear . . . Of course they're open

What's the maximum amount per person? Isn't there another way to make larger donations?

We talked about this recently. 2500 per person.

I understand

Yes

Can someone make a donation to NYC? 200-300K etc.

It happens . . . But it has to be companies here

There are some

They can't accept it from outside

A U.S. company need to make the donation . . . Can we talk some time?

21. I have also reviewed records obtained pursuant to a search warrant for an iCloud account used by [REDACTED] who as discussed above was an employee of [REDACTED] stationed in New York City who was involved in assisting Adams with travel to Turkey in coordination with [REDACTED] and [REDACTED] the Consul General discussed above. On April 13, 2019, [REDACTED] wrote [REDACTED] in an effort to arrange a meeting, stating in part "We've been in contact with regard to Eric Adams before." On January 11, 2022, [REDACTED] again attempted to arrange a meeting with [REDACTED] and wrote in part "We talked to each other during Eric Adams' visits to Turkey, if you recall."

The FDNY and the TCO

22. I have reviewed emails sent by FDNY employees from their official FDNY email accounts, which were obtained by the New York City Department of Investigations ("DOI"). Those emails revealed, in substance and in part, that shortly before Adams' involvement in the

Turkish Consulate General's receipt of the TCO discussed above, the Consulate General was requesting the TCO on an urgent basis, without success, because the FDNY would not concur due to concerns about the building's fire safety systems. Once Adams' involvement began (as reflected in his messages with [REDACTED] discussed above, and further discussed below) however, the TCO was issued, without the FDNY actually inspecting the location and despite concerns that this omission was unsafe.

23. I have spoken with an FBI agent who interviewed an FDNY Assistant Chief who was the FDNY Chief of Fire Prevention at the time the above TCO was issued (the "Fire Prevention Chief"), and reviewed a report of that interview. In substance and in part, the Fire Prevention Chief stated that he received requests from multiple New York City officials to concur in the issuance of a TCO for the Turkish Consulate building for over one week prior to September 10, 2021. The Fire Prevention Chief had been unwilling to agree to issuance of the TCO because, in substance, he was not satisfied with the adequacy of the fire prevention systems in the building. On the afternoon of September 10, 2021, however, FDNY's Chief of Department (the senior uniformed member of the FDNY) told the Fire Prevention Chief that it was important for the TCO to issue, and that he and the Fire Prevention Chief would lose their jobs if it did not. The Chief of Fire Prevention understood the pressure to facilitate the TCO to be coming from the Adams Campaign. The Fire Prevention Chief issued a letter which did not conform to FDNY standards but was sufficient for the New York City Department of Buildings to issue the TCO. As discussed above, on the afternoon of September 10, 2021, [REDACTED] relayed to Adams [REDACTED]'s request that Adams intervene in this matter and Adams appeared to inform [REDACTED] that he was speaking with FDNY personnel to "resolve" the matter.

24. I have spoken with the Chief of Department, whose recollection of the events on September 10, 2021 was less detailed than, but not inconsistent with, the account of the Fire Prevention Chief.

25. I have spoken with an FBI agent who interviewed an individual who was the FDNY Commissioner, an appointed position senior to the Chief of Department (the “Commissioner”), in September 2021, and reviewed a report of that interview. The Commissioner stated, in substance and in part, that he had a vague memory of efforts by the Turkish General Consulate to obtain a TCO in early September 2021, and may have spoken with the Chief of Department or Fire Prevention Chief about it, but did not recall specific details, although at the time he was pre-occupied with the 20th anniversary commemoration of the 9/11 attacks. The Commissioner did not recall speaking to Adams about it, or having ever spoken to Adams with the exception of social interactions at public events.

26. I have reviewed records of electronic messages between Adams and the Commissioner exchanged between August 3, 2021 and January 5, 2022, found on the Adams iCloud Account. These messages began with the Commissioner introducing himself to Adams and asking to be considered to remain as Commissioner, touting himself as “loyal and trustworthy.” In messages exchanged between September 8, 2021 and September 10, 2021, Adams requested, in substance, that the Commissioner intervene to ensure that the FDNY issue the letter required to obtain the TCO. As of the morning of September 10, 2021, Adams informed the Commissioner that this had not yet been done. At approximately 12:44 p.m. that day the Commissioner told Adams that he was “working on that as we speak,” and at approximately 2:17 p.m. the Commissioner informed Adams “Letter being drafted now. Everything should be good to go Monday morning.”

B. Probable Cause Justifying Search of the Subject Premises

27. I know, based on my review of Amazon records, that there are two Amazon accounts in [REDACTED] name (using two different email addresses), and that the Subject Premises was entered as a delivery address on one of the accounts in February 2021, and was entered as a delivery address on the other account in October 2022. Amazon records also indicate that [REDACTED] added a credit card to her Amazon account in or about December 2022, using the Subject Premises as her billing address. Records received in July 2022 from an information technology company to which [REDACTED] devices are subscribed, and records accessed in July 2023 from the New York Department of Mobile Vehicles, likewise reflect that [REDACTED] [REDACTED] resides at the Subject Premises.

28. Based on my review of property records for the Subject Premises, I know that the Subject Premises is owned by [REDACTED], [REDACTED], and [REDACTED], the three of whom were listed as borrowers on a March 8, 2022 mortgage that property records do not indicate has been satisfied.

29. Based on my discussions with an officer with the New York City Police Department (“NYPD”), I know that on the evening of November 1, 2023, officers with the NYPD attempted to conduct a wellness check at the subject premises. When the officers arrived, the lights of the Subject Premises were off and no one was home. However, shortly after the officers arrived at the Subject Premises, a man walked up to the officers. The man identified himself as [REDACTED] [REDACTED] told the officers, in substance and in part, that the Subject Premises is a single-family home, and that although he does not live there, his daughter [REDACTED], and her grandmother [REDACTED], do live there.

30. Based on my training and experience, persons generally keep their cellphones, laptops, and tablets (such as iPads) accessible, meaning that if a person is home, those devices are likely to be in their residence. I am aware, including based on the communications described above,

that [REDACTED] used electronic communications in furtherance of the Subject Offenses. Based on my training and experience, electronic communications, including emails and text messages, are frequently stored on persons' cellphones, laptops, and tablets. In addition, based on my training and experience and my involvement in this investigation, I know that persons often receive financial records, including bank and credit card statements that may reflect the provision or receipt of pecuniary benefits, by mail to their residence.

C. Probable Cause Justifying Search of ESI

31. For the reasons set forth above, there is probable cause to believe that cellphones, tablets (including Apple iPads), and computers used by [REDACTED] will contain evidence of the Subject Offenses. In addition to the evidence discussed above that [REDACTED] has used such devices to communicate about the Subject Offenses,¹⁵ there is probable cause to believe that cellphones, tablets (including Apple iPads), and computers used [REDACTED] will contain evidence of the Subject Offenses for these additional reasons:

a. Computers, tablets, and cellphones can be used store documents, including emails, text messages, previous electronic chats, and financial documents like bank statements and travel expenditure. Tablets and computers can also be used to create documents in word processing programs, like Microsoft Word. Document attachments to communications can be saved intentionally or as a result of a cellphone's or tablet's operating system or web browser to an electronic device, including a computer, tablet, or cellphone. Moreover, and more generally, users of cellphones, tablets, and computers who are engaged in the commission of the Subject Offenses

¹⁵ As noted above, some of the relevant communications were recovered from [REDACTED]'s iCloud account. Based on my training and experience, iCloud backups often contain a subset of the information contained on the electronic device that is backed up. As a result, there is probable cause to believe that the communications already recovered from [REDACTED]'s iCloud account, as well as additional evidence, will be found on [REDACTED]'s electronic devices.

often store documents relevant to that activity on their devices, and also maintain notes of meetings and telephone calls on their devices. Such documents can include, but are not limited to, Microsoft Word and PDF documents, drafts, scans, bank statements received from financial institutions, and government filings.

b. Cellphones, tablets, and computers can contain photographs and videos of meetings—such as the images of [REDACTED] with Adams and [REDACTED] discussed above—and documents, audio recordings of telephone calls and meetings, and screenshots of text messages.

c. Electronic files, or remnants of those files, downloaded to a cellphone, tablet, or computer can be stored for years at little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily available forensics tools. When a person “deletes” a file on a cellphone, tablet, or computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium and within the device unless and until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the device that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space—for long periods of time before they are overwritten. In addition, a device’s operating system may also keep a record of deleted data in a “swap” or “recovery” file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or “cache.” The browser typically maintains a fixed amount of electronic storage medium space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve “residue” of an electronic file from a cellphone, tablet, or computer depends less on when the file was downloaded or viewed than on a particular user’s operating system, storage capacity, and cellphone habits.

d. Additionally, a person can transfer data from an old cellphone, tablet, or computer to a new device, including, for example, mail, contacts, calendars, photos and videos, books and pdfs, call logs, and text messages. For individuals who regularly change or upgrade their devices, including cellphones, it is common to transfer electronic records, such as emails, contacts, calendars, photos and videos, books and pdfs, call logs, and text messages from the old phone to a new phone. Individuals can transfer data in a few ways, including in a cellphone provider or Apple store, through a personal computer containing a backup, or through an iCloud backup. Accordingly, data found on one electronic device is often found on other devices used by the same person.

e. Accordingly, there is probable cause to believe that evidence, fruits, and instrumentalities of the Subject Offenses listed in Attachment B, which is incorporated by reference herein, will be found in the Subject Premises, and on electronic devices found in the Subject Premises.

32. Based on my training and experience, I also know that, where computers are used in furtherance of criminal activity, evidence of the criminal activity can often be found months or even years after it occurred. This is typically true because:

- Electronic files can be stored on a hard drive for years at little or no cost and users thus have little incentive to delete data that may be useful to consult in the future.
- Even when a user does choose to delete data, the data can often be recovered months or years later with the appropriate forensic tools. When a file is “deleted” on a home computer, the data contained in the file does not actually disappear, but instead remains on the hard drive, in “slack space,” until it is overwritten by new data that cannot be stored elsewhere on the computer. Similarly, files that have been viewed on the Internet are generally downloaded into a temporary Internet directory or “cache,” which is only overwritten as the “cache” fills up and is replaced with more recently viewed Internet pages. Thus, the ability to retrieve from a hard drive or other electronic storage media depends less on when the file was created or viewed than on a particular user’s operating system, storage capacity, and computer habits.

- In the event that a user changes computers, the user will typically transfer files from the old computer to the new computer, so as not to lose data. In addition, users often keep backups of their data on electronic storage media such as thumb drives, flash memory cards, CD-ROMs, or portable hard drives.

33. Based on the foregoing, I respectfully submit there is probable cause to believe that [REDACTED] has committed the Subject Offenses, and that evidence of this criminal activity is likely to be found in the Subject Premises and on computers and electronic media found in the Subject Premises.

III. Procedures for Searching ESI

A. Execution of Warrant for ESI

34. Federal Rule of Criminal Procedure 41(e)(2)(B) provides that a warrant to search for and seize property “may authorize the seizure of electronic storage media or the seizure or copying of electronically stored information . . . for later review.” Consistent with Rule 41, this application requests authorization to seize any computer devices and storage media and transport them to an appropriate law enforcement facility for review. This is typically necessary for a number of reasons:

- First, the volume of data on computer devices and storage media is often impractical for law enforcement personnel to review in its entirety at the search location.
- Second, because computer data is particularly vulnerable to inadvertent or intentional modification or destruction, computer devices are ideally examined in a controlled environment, such as a law enforcement laboratory, where trained personnel, using specialized software, can make a forensic copy of the storage media that can be subsequently reviewed in a manner that does not change the underlying data.
- Third, there are so many types of computer hardware and software in use today that it can be impossible to bring to the search site all of the necessary technical manuals and specialized personnel and equipment potentially required to safely access the underlying computer data.
- Fourth, many factors can complicate and prolong recovery of data from a computer device, including the increasingly common use of passwords, encryption, or other features or configurations designed to protect or conceal data on the computer, which often take considerable time and resources for forensic personnel to detect and resolve.

B. Accessing ESI

35. I know from my training and experience, as well as from information found in publicly available materials, that Apple iPhones and iPads offer their users the ability to unlock the device via biometric features (e.g., fingerprint, facial recognition) in lieu of a numeric or alphanumeric passcode or password. Apple's fingerprint recognition feature is called Touch ID, and its facial recognition feature is called Face ID.

36. If a user enables Touch ID on a given device, he or she can register up to 5 fingerprints that can be used to unlock that device. The user can then use any of the registered fingerprints to unlock the device by pressing the relevant finger(s) to the device's Touch ID sensor, which is found in the round button (often referred to as the "home" button) found at the bottom center of the front of the device.

37. If a user enables Face ID on a given device, he or she can unlock the device by raising the iPhone to his or her face.

38. In my training and experience, users of devices that offer Touch ID or Face ID often enable it because it is considered to be a more convenient way to unlock the device than by entering a numeric or alphanumeric passcode or password, as well as a more secure way to protect the device's contents.

39. In some circumstances, Touch ID or Face ID cannot be used to unlock a device that has either security feature enabled, and a passcode or password must be used instead. These circumstances include: (1) when the device has just been turned on or restarted; (2) when more than 48 hours has passed since the last time the device was unlocked; (3) when the passcode or password has not been entered in the last 6 days, and the device has not been unlocked via Touch ID in the last 8 hours or the device has not been unlocked via Face ID in the last 4 hours; (4) the

device has received a remote lock command; or (5) five unsuccessful attempts to unlock the device via Touch ID or Face ID are made.

40. The passcodes or passwords that would unlock electronic devices subject to seizure pursuant to the requested warrant are unknown to law enforcement. Thus, it will likely be necessary to press [REDACTED] fingers to any Touch ID sensors, or to hold those devices in front of [REDACTED] face to activate the Face ID sensor, in an attempt to unlock those devices for the purpose of executing the search authorized by this warrant. Attempting to unlock the relevant devices via Touch ID with the use of the fingerprint of the user, or via Face ID by holding the device in front of the user's face, is necessary because the government may not otherwise be able to access the data contained on those devices for the purpose of executing the search authorized by this warrant.

41. Although I do not know which of a given user's 10 fingerprints are capable of unlocking a particular device, based on my training and experience I know that it is common for a user to unlock a Touch ID-enabled device via the fingerprints on thumbs or index fingers. In the event that law enforcement is unable to unlock any electronic devices as described above within the five attempts permitted by Touch ID, this will simply result in the device requiring the entry of a password or passcode before it can be unlocked.

42. I also know from my training and experience, and my review of publicly available materials that Apple brand devices have a feature that allows a user to erase the contents of the device remotely. By logging into the Internet, the user or any other individual who possesses the user's account information can take steps to completely wipe the contents of the device, thereby destroying evidence of criminal conduct, along with any other information on the device. The only means to prevent this action is to disable the device's ability to connect to the Internet

immediately upon seizure, which requires either access to the device itself to alter the settings, or the use of specialized equipment that is not consistently available to law enforcement agents.

43. Due to the foregoing, I request that the Court authorize law enforcement to press [REDACTED] (including thumbs) to the Touch ID of any seized devices, or to hold those devices in front of [REDACTED] face (and, if necessary, to hold [REDACTED] in place while holding the electronic devices in front of his face), for the purpose of attempting to unlock the devices via Touch ID or Face ID in order to search the contents as authorized by this warrant.

C. Review of ESI

44. Following seizure of any computer devices and storage media and/or the creation of forensic image copies, law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) will review the ESI contained therein for information responsive to the warrant.

45. In conducting this review, law enforcement personnel may use various techniques to determine which files or other ESI contain evidence or fruits of the Subject Offenses. Such techniques may include, for example:

- surveying directories or folders and the individual files they contain (analogous to looking at the outside of a file cabinet for the markings it contains and opening a drawer believed to contain pertinent files);
- conducting a file-by-file review by “opening” or reading the first few “pages” of such files in order to determine their precise contents (analogous to performing a cursory examination of each document in a file cabinet to determine its relevance);
- “scanning” storage areas to discover and possibly recover recently deleted data or deliberately hidden files; and

- performing electronic keyword searches through all electronic storage areas to determine the existence and location of data potentially related to the subject matter of the investigation¹⁶; and
- reviewing metadata, system information, configuration files, registry data, and any other information reflecting how, when, and by whom the computer was used.

46. Law enforcement personnel will make reasonable efforts to restrict their search to data falling within the categories of evidence specified in the warrant. Depending on the circumstances, however, law enforcement personnel may need to conduct a complete review of all the ESI from seized devices or storage media to evaluate its contents and to locate all data responsive to the warrant.

D. Return of ESI

47. If the Government determines that the electronic devices are no longer necessary to retrieve and preserve the data, and the devices themselves are not subject to seizure pursuant to Federal Rule of Criminal Procedure 41(c), the Government will return these items. Computer data that is encrypted or unreadable will not be returned unless law enforcement personnel have determined that the data is not (i) an instrumentality of the offense, (ii) a fruit of the criminal activity, (iii) contraband, (iv) otherwise unlawfully possessed, or (v) evidence of the Subject Offenses.

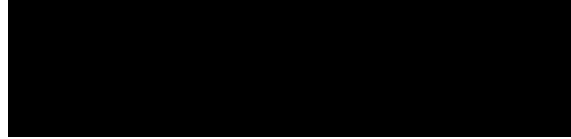
¹⁶ Keyword searches alone are typically inadequate to detect all relevant data. For one thing, keyword searches work only for text data, yet many types of files, such as images and videos, do not store data as searchable text. Moreover, even as to text data, there may be information properly subject to seizure but that is not captured by a keyword search because the information does not contain the keywords being searched.

IV. Conclusion and Ancillary Provisions

48. Based on the foregoing, I respectfully request the court to issue a warrant to search the Subject Premises described in Attachment A, and to seize the items and information specified in Attachment B, to this affidavit and to the Search and Seizure Warrant.

49. The existence and scope of this ongoing criminal investigation is not publicly known. Although the execution of the requested warrant will reveal to [REDACTED] the general existence of an investigation into the Subject Offenses, it will not reveal its full scope, including the witnesses and evidence discussed in this affidavit. Premature public disclosure of this affidavit could cause [REDACTED] and her associates and co-conspirators to destroy evidence not yet gathered by law enforcement, much of which likely exists in electronic or paper forms that can be readily destroyed. In addition, disclosure of this affidavit could cause the subjects of this investigation to believe that their arrest is imminent, triggering their flight. That is especially concerning given that some of the subjects of the investigation discussed herein have significant ties abroad (as partly discussed in this affidavit), and regularly travel abroad. For these reasons, I respectfully request that this affidavit and all papers submitted herewith be maintained under seal until the Court orders otherwise, except that the Government be permitted without further order of this Court to provide copies of the warrant and affidavit as needed to personnel assisting in the investigation and

prosecution of this matter, and to disclose those materials as necessary to comply with discovery and disclosure obligations in any prosecutions related to this matter.



Special Agent
Federal Bureau of Investigation

Sworn to me through the transmission of this
Affidavit by reliable electronic means, pursuant to
Federal Rules of Criminal Procedure 41(d)(3) and 4.1, this

November 1, 2023

Lois Bloom

HON. LOIS BLOOM
UNITED STATES MAGISTRATE JUDGE
EASTERN DISTRICT OF NEW YORK

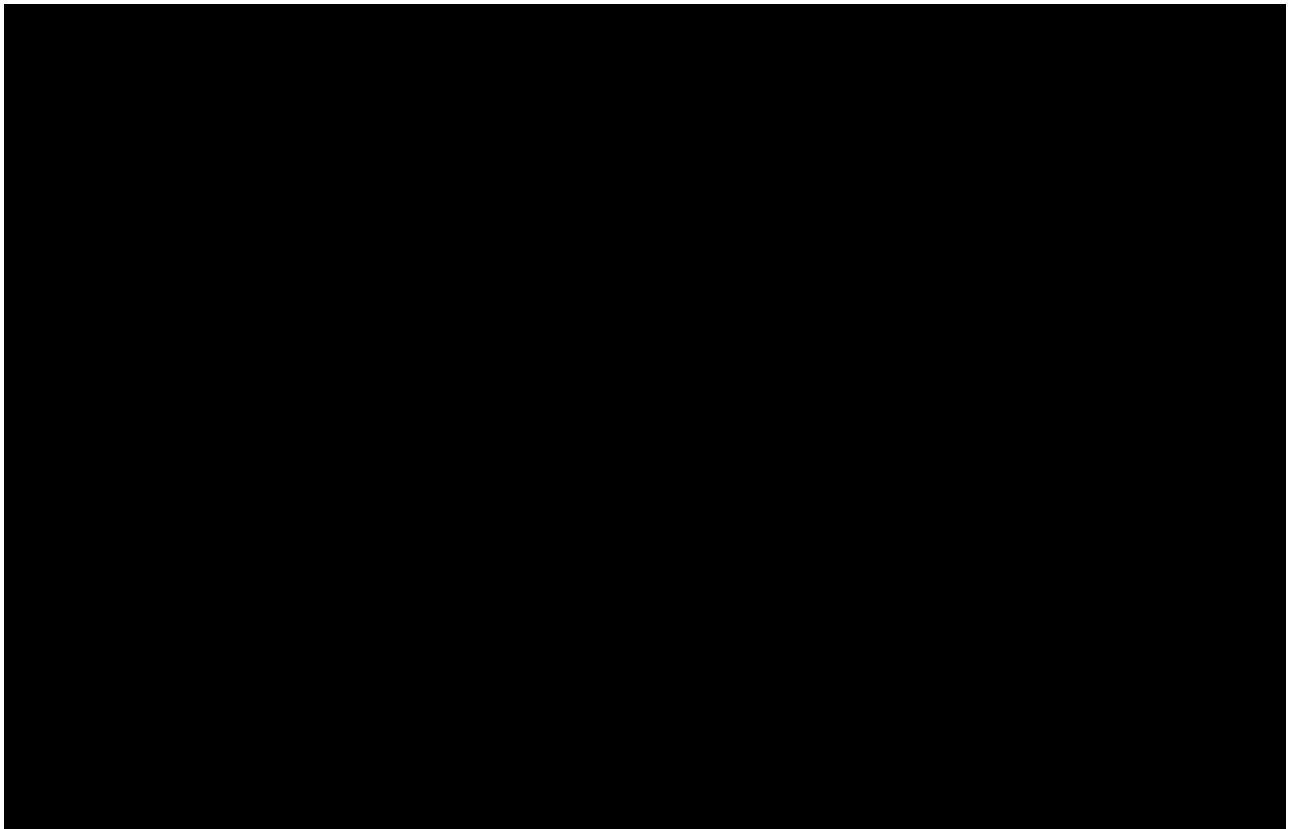
ATTACHMENT A

Premises to be Searched—Subject Premises

The premises to be searched (the “Subject Premises”) are described as follows, and include all locked and closed containers found therein:

The Subject Premises is particularly described as [REDACTED], Brooklyn, New York 11213.

[REDACTED] is a three-story limestone building, accessed via windowed double doors up a flight of stairs from the sidewalk, with the number “[REDACTED]” inscribed on a diagonal to the left of the doors. The building, and a close-up of the doorway to the Subject Premises, are depicted below.



ATTACHMENT B

Items to Be Seized

A. Evidence, Fruits, and Instrumentalities of the Subject Offenses

The items to be seized from the Subject Premises consist of the following evidence, fruits, and instrumentalities of violations of (i) 18 U.S.C. §§ 371 and 666 (theft of federal funds and conspiracy to steal federal funds), (ii) 18 U.S.C. §§ 1343 and 1349 (wire fraud and attempt and conspiracy to commit wire fraud), and (iii) 18 U.S.C. § 371 and 52 U.S.C. § 30121 (campaign contributions by foreign nationals and conspiracy to commit the same) (collectively, the “Subject Offenses”), described as follows:

1. Evidence concerning occupancy or ownership of the Subject Premises, including without limitation, utility and telephone bills, mail envelopes, addressed correspondence, diaries, statements, identification documents, address books, telephone directories, and keys.
2. Financial records for [REDACTED] and any entity controlled by or associated with [REDACTED]
3. Documents related to contributions to the 2021 New York City mayoral campaign of Eric Adams (the “Adams Campaign”).
4. Documents related to travel to Turkey by any employee, officer, or associate of the Adams Campaign.
5. Documents related to interactions between the Adams Campaign and the Government of Turkey, including persons acting at the behest of the Turkish Government.
6. Electronic devices, including cellphones, laptops, and tablets, owned or used by [REDACTED] (hereinafter, the “Seized Devices”).
7. Evidence regarding the identity of the owner or user of the Seized Devices at times relevant to the Subject Offenses.

The Seized Devices may be searched for the following evidence, fruits, and instrumentalities of the Subject Offenses:

A. Evidence of knowledge or understanding of, or intent to violate, laws and regulations governing the conduct of the 2021 New York City Mayoral campaign on the part of [REDACTED] and its employees, officers, or associates (“[REDACTED]”); the Turkish Government, including its Consulate General in New York and its employees, officers, or associates; or the Adams Campaign.

B. Evidence relating to coordination between [REDACTED], Turkish nationals, or the Turkish Government and the Adams Campaign concerning political contributions to the Adams Campaign, including, but not limited to, evidence of motive and intent for [REDACTED], Turkish nationals, or the Turkish Government to provide or facilitate campaign contributions to the Adams Campaign, and

evidence of motive and intent by any person who is or was associated with or employed by the Adams Campaign to provide benefits, whether lawfully or unlawfully, to [REDACTED], Turkish nationals, or the Turkish Government in return for campaign contributions.

C. Evidence relating to payments to employees, officers, and associates of [REDACTED] to facilitate those employees, officers, and associates making campaign contributions to the Adams Campaign.

D. Evidence relating to the source of funds for payment or reimbursement of employees, officers, and associates of [REDACTED] or other persons serving as conduits for campaign contributions to the Adams Campaign originating from Turkish nationals.

E. Evidence of individuals or entities who donated to the Adams Campaign before or after receiving transfers of funds similar to the amount of the donation.

F. Evidence regarding the identity of any persons or entities involved, wittingly or unwittingly, in straw donations to the Adams Campaign.

G. Evidence of the relationship between and among [REDACTED], the Turkish Government, or Turkish nationals covertly contributing to the Adams campaign or any person who is or was associated with or employed by the Adams Campaign, including all communications with or about, contact information for, and meetings and appointments with co-conspirators.

H. Evidence of an intent to exchange benefits between the Turkish Government or entities and persons acting at its behest, and any person who is or was associated with or employed by the Adams Campaign, including but not limited to straw donations and any actions taken by any person who is or was associated with or employed by the Adams Campaign on behalf of the Turkish Government, [REDACTED], or entities and persons acting at the behest of the Turkish Government.

I. Evidence regarding any requests by the Adams Campaign for matching funds based on donations from [REDACTED] personnel, or any other straw donors, including any discussions of matching funds.

J. Passwords or other information needed to access the user's online accounts, including encrypted data stored in the Seized Devices.

K. Evidence sufficient to establish the owners and users of the Seized Devices at times relevant to the Subject Offenses.

L. Evidence of the geographic location of users, computers, or devices involved in the commission of the Subject Offenses at times relevant to the Subject Offenses.

B. Search and Seizure of Electronically Stored Information

The items to be seized from the Subject Premises also include any computer devices and storage media that may contain any electronically stored information falling within the categories set forth in Section A of this Attachment above, including, but not limited to, desktop and laptop

computers, cellphones, and tablets (including iPads). In lieu of seizing any such computer devices or storage media, this warrant also authorizes the copying of such devices or media for later review.

Included within the items to be seized from the Subject Premises are:

1. Any items or records needed to access the data stored on any seized or copied computer devices or storage media, including but not limited to any physical keys, encryption devices, or records of login credentials, passwords, private encryption keys, or similar information.
2. Any items or records that may facilitate a forensic examination of the computer devices or storage media, including any hardware or software manuals or other information concerning the configuration of the seized or copied computer devices or storage media.
3. Any evidence concerning the identities or locations of those persons with access to, control over, or ownership of the seized or copied computer devices or storage media.

C. Accessing ESI

During execution of the search of the Subject Premises authorized herein, law enforcement personnel are authorized to (1) press or swipe the fingers (including thumbs) of [REDACTED] to any device found at the premises reasonably believed by law enforcement to be used by [REDACTED]; (2) hold any such device in front of [REDACTED]'s face and activate the facial recognition feature, for the purpose of attempting to unlock the device in order to search the contents as authorized by this warrant.

D. Review of ESI

Following seizure of any computer devices and storage media and/or the creation of forensic image copies, law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review the ESI contained therein for information responsive to the warrant.

In conducting this review, law enforcement personnel may use various techniques to locate information responsive to the warrant, including, for example:

- surveying various file “directories” and the individual files they contain (analogous to looking at the outside of a file cabinet for the markings it contains and opening a drawer believed to contain pertinent files);
- opening or cursorily reading the first few “pages” of such files in order to determine their precise contents;
- scanning storage areas to discover and possibly recover recently deleted files or deliberately hidden files;

- performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are intimately related to the subject matter of the investigation; and
- reviewing metadata, system information, configuration files, registry data, and any other information reflecting how, when, and by whom the computer was used.

Law enforcement personnel will make reasonable efforts to search only for files, documents, or other electronically stored information within the categories identified in Sections A and B of this Attachment. However, law enforcement personnel are authorized to conduct a complete review of all the ESI from seized devices or storage media if necessary to evaluate its contents and to locate all data responsive to the warrant.

SDNY_01_000004564
SUBJECT TO PROTECTIVE ORDER.

AO 93 (Rev. 11/13) Search and Seizure Warrant (Page 2)

Return

Case No.:

23-MJ-967

Date and time warrant executed:

Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

*Executing officer's signature*_____
Printed name and title

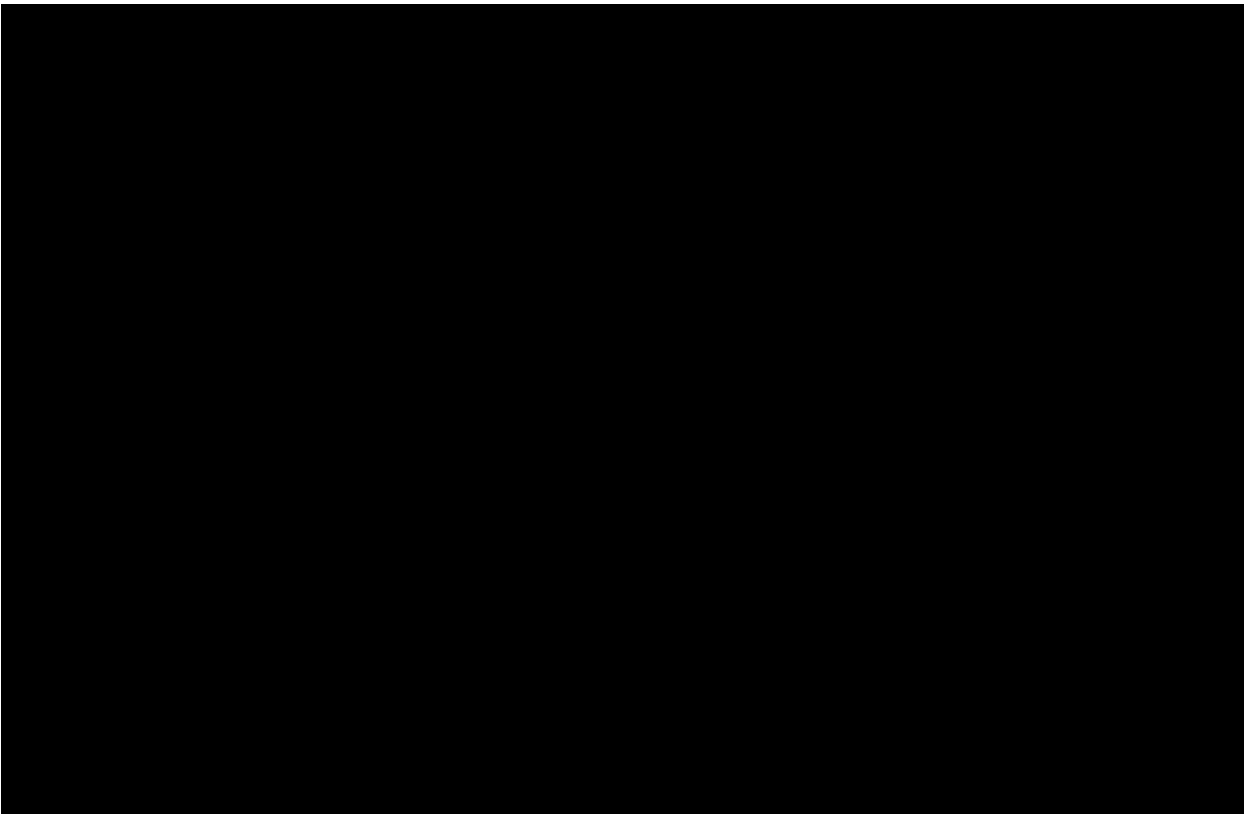
ATTACHMENT A

Premises to be Searched—Subject Premises

The premises to be searched (the “Subject Premises”) are described as follows, and include all locked and closed containers found therein:

The Subject Premises is particularly described as [REDACTED], Brooklyn, New York 11213.

[REDACTED] is a three-story limestone building, accessed via windowed double doors up a flight of stairs from the sidewalk, with the number “[REDACTED]” inscribed on a diagonal to the left of the doors. The building, and a close-up of the doorway to the Subject Premises, are depicted below.



ATTACHMENT B

Items to Be Seized

A. Evidence, Fruits, and Instrumentalities of the Subject Offenses

The items to be seized from the Subject Premises consist of the following evidence, fruits, and instrumentalities of violations of (i) 18 U.S.C. §§ 371 and 666 (theft of federal funds and conspiracy to steal federal funds), (ii) 18 U.S.C. §§ 1343 and 1349 (wire fraud and attempt and conspiracy to commit wire fraud), and (iii) 18 U.S.C. § 371 and 52 U.S.C. § 30121 (campaign contributions by foreign nationals and conspiracy to commit the same) (collectively, the “Subject Offenses”), described as follows:

1. Evidence concerning occupancy or ownership of the Subject Premises, including without limitation, utility and telephone bills, mail envelopes, addressed correspondence, diaries, statements, identification documents, address books, telephone directories, and keys.
2. Financial records for [REDACTED] and any entity controlled by or associated with [REDACTED]
3. Documents related to contributions to the 2021 New York City mayoral campaign of Eric Adams (the “Adams Campaign”).
4. Documents related to travel to Turkey by any employee, officer, or associate of the Adams Campaign.
5. Documents related to interactions between the Adams Campaign and the Government of Turkey, including persons acting at the behest of the Turkish Government.
6. Electronic devices, including cellphones, laptops, and tablets, owned or used by [REDACTED] (hereinafter, the “Seized Devices”).
7. Evidence regarding the identity of the owner or user of the Seized Devices at times relevant to the Subject Offenses.

The Seized Devices may be searched for the following evidence, fruits, and instrumentalities of the Subject Offenses:

A. Evidence of knowledge or understanding of, or intent to violate, laws and regulations governing the conduct of the 2021 New York City Mayoral campaign on the part of [REDACTED] and its employees, officers, or associates (“[REDACTED]”); the Turkish Government, including its Consulate General in New York and its employees, officers, or associates; or the Adams Campaign.

B. Evidence relating to coordination between [REDACTED], Turkish nationals, or the Turkish Government and the Adams Campaign concerning political contributions to the Adams Campaign, including, but not limited to, evidence of motive and intent for [REDACTED], Turkish nationals, or the Turkish Government to provide or facilitate campaign contributions to the Adams Campaign, and

evidence of motive and intent by any person who is or was associated with or employed by the Adams Campaign to provide benefits, whether lawfully or unlawfully, to [REDACTED], Turkish nationals, or the Turkish Government in return for campaign contributions.

C. Evidence relating to payments to employees, officers, and associates of [REDACTED] to facilitate those employees, officers, and associates making campaign contributions to the Adams Campaign.

D. Evidence relating to the source of funds for payment or reimbursement of employees, officers, and associates of [REDACTED] or other persons serving as conduits for campaign contributions to the Adams Campaign originating from Turkish nationals.

E. Evidence of individuals or entities who donated to the Adams Campaign before or after receiving transfers of funds similar to the amount of the donation.

F. Evidence regarding the identity of any persons or entities involved, wittingly or unwittingly, in straw donations to the Adams Campaign.

G. Evidence of the relationship between and among [REDACTED], the Turkish Government, or Turkish nationals covertly contributing to the Adams campaign or any person who is or was associated with or employed by the Adams Campaign, including all communications with or about, contact information for, and meetings and appointments with co-conspirators.

H. Evidence of an intent to exchange benefits between the Turkish Government or entities and persons acting at its behest, and any person who is or was associated with or employed by the Adams Campaign, including but not limited to straw donations and any actions taken by any person who is or was associated with or employed by the Adams Campaign on behalf of the Turkish Government, [REDACTED], or entities and persons acting at the behest of the Turkish Government.

I. Evidence regarding any requests by the Adams Campaign for matching funds based on donations from [REDACTED] personnel, or any other straw donors, including any discussions of matching funds.

J. Passwords or other information needed to access the user's online accounts, including encrypted data stored in the Seized Devices.

K. Evidence sufficient to establish the owners and users of the Seized Devices at times relevant to the Subject Offenses.

L. Evidence of the geographic location of users, computers, or devices involved in the commission of the Subject Offenses at times relevant to the Subject Offenses.

B. Search and Seizure of Electronically Stored Information

The items to be seized from the Subject Premises also include any computer devices and storage media that may contain any electronically stored information falling within the categories set forth in Section A of this Attachment above, including, but not limited to, desktop and laptop

computers, cellphones, and tablets (including iPads). In lieu of seizing any such computer devices or storage media, this warrant also authorizes the copying of such devices or media for later review.

Included within the items to be seized from the Subject Premises are:

1. Any items or records needed to access the data stored on any seized or copied computer devices or storage media, including but not limited to any physical keys, encryption devices, or records of login credentials, passwords, private encryption keys, or similar information.
2. Any items or records that may facilitate a forensic examination of the computer devices or storage media, including any hardware or software manuals or other information concerning the configuration of the seized or copied computer devices or storage media.
3. Any evidence concerning the identities or locations of those persons with access to, control over, or ownership of the seized or copied computer devices or storage media.

C. Accessing ESI

During execution of the search of the Subject Premises authorized herein, law enforcement personnel are authorized to (1) press or swipe the fingers (including thumbs) of [REDACTED] to any device found at the premises reasonably believed by law enforcement to be used by [REDACTED] (2) hold any such device in front of [REDACTED] face and activate the facial recognition feature, for the purpose of attempting to unlock the device in order to search the contents as authorized by this warrant.

D. Review of ESI

Following seizure of any computer devices and storage media and/or the creation of forensic image copies, law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review the ESI contained therein for information responsive to the warrant.

In conducting this review, law enforcement personnel may use various techniques to locate information responsive to the warrant, including, for example:

- surveying various file “directories” and the individual files they contain (analogous to looking at the outside of a file cabinet for the markings it contains and opening a drawer believed to contain pertinent files);
- opening or cursorily reading the first few “pages” of such files in order to determine their precise contents;
- scanning storage areas to discover and possibly recover recently deleted files or deliberately hidden files;

- performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are intimately related to the subject matter of the investigation; and
- reviewing metadata, system information, configuration files, registry data, and any other information reflecting how, when, and by whom the computer was used.

Law enforcement personnel will make reasonable efforts to search only for files, documents, or other electronically stored information within the categories identified in Sections A and B of this Attachment. However, law enforcement personnel are authorized to conduct a complete review of all the ESI from seized devices or storage media if necessary to evaluate its contents and to locate all data responsive to the warrant.